UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

GARY GRAIFMAN, on behalf of himself and all others similarly situated, Plaintiff, v. CHRISTIE'S INC., Defendant.	Civil Action No. _____ **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff, Gary Graifman ("Plaintiff"), individually and on behalf of all others similarly situated, brings this Class Action Complaint against Christie's Inc. ("Christie's" or "Defendant"), and alleges, upon personal knowledge as to his own actions and the investigation of counsel, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Plaintiff brings this action to remedy harms inflicted by Defendant in failing to properly secure and safeguard Plaintiff's and Class Members' sensitive Personal Identifiable Information ("PII").

2. On May 30, 2024, Plaintiff received an email (the "Data Breach Notice") from Defendant which stated, *inter alia,* that "an unauthorized third party had. . . downloaded. . . information relating to client ID checks, which [Christie's is] required to retain for compliance reasons."

3. The infiltration of Defendant's unsecured network and the theft of customers' sensitive PII (the "Data Breach") was discovered on May 9, 2024. No information has been provided as to how the cybercriminals illegally accessed Defendant's network, and access to Defendant's website was disrupted for a period of ten days following the discovery of the breach.

4. On May 27, 2024, the criminal ransomware group Ransomhub announced that it had acquired two gigabytes of sensitive personal information for 500,000 private clients of Defendant and included screenshots as proof.[1] The group threatened to leak the information if Defendant did not pay a ransom for the information.[2]

5. Ransomhub accused Defendant of breaking off negotiations after Ransomhub attempted "to come to a reasonable conclusion."[3] Ransomhub stated that "It is clear that if this information is posted [Christie's] will incur heavy fines from GDPR as well as ruining their reputation with their clients and [Christie's does not] care about their privacy."[4]

---

[1] *Christie's Auction House Confirms Data Breach after Ransomware Group Threatens to Leak Stolen Info*, CPO Magazine (Jun. 4, 2024), https://www.cpomagazine.com/cyber-security/christies-auction-house-confirms-data-breach-after-ransomware-group-threatens-to-leak-stolen-info/.

[2] *Id.*

[3] *Id.*

[4] *Id.* "GDPR" refers to the European Union's Data Protection Law Enforcement Directive (https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en).

6. As Defendant refused to pay the ransom for its customers' sensitive information, Ransomhub subsequently announced that it sold the data to the highest bidder on its dark web leak site.[5] Ransomhub's announcement confirmed that Plaintiff's and Class Members' PII is now in the hands of criminals who will use the information to commit further crimes.

7. Defendant confirmed in its Data Breach Notice that the stolen PII included, among other things, Plaintiff's and Class Members' full names, dates of birth, home countries, and the document numbers of their identifying documents including, but not limited to, drivers' licenses. The screenshots posted by Ransomhub show that the PII also included phenotype information displayed on Plaintiff's and Class Members' identifying documents.

8. Defendant's failure to secure and protect its customers' PII places Plaintiff and Class Members at heightened, imminent, and permanent risk of fraud and identity theft. Plaintiff and Class Members have also lost the benefit of their bargain, out-of-pocket expenses incurred to mitigate the effects of the Data Breach, and the value of their time reasonably incurred to mitigate the effects of the Data Breach. Plaintiff and Class Members have suffered concrete injuries in fact including, but not limited to: (i) invasion of privacy; (ii) theft of their sensitive PII;

[5] Daniel Croft, *Christie's data auctioned off to highest bidder after ransom refused*, cyberdaily.au (Jun. 7, 2024) https://www.cyberdaily.au/security/10677-christies-data-auctioned-off-to-highest-bidder-after-ransom-refused.

(iii) lost or diminished value of their PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails and attempts to open fraudulent accounts; (viii) statutory damages; (ix) nominal damages; and (x) the continued and increased risk to their PII, which remains unencrypted and available for unauthorized third parties to further access and abuse, in addition to remaining backed up in Defendant's possession and subject to further unauthorized disclosure so long as Defendant fails to undertake necessary and appropriate measures to protect its customers' private information.

9. Given the frequency of cyberattacks in the past several years, Defendant knew or had reason to know that it would be targeted by cybercriminals attempting to access the valuable information that it retained from its wealthy clientele. The Data Breach was a foreseeable and avoidable danger that Defendant failed to take reasonable steps to prevent.

10. Therefore, Plaintiff brings this suit on behalf of himself and all similarly situated individuals for negligence, negligence per se, breach of contract, breach of implied contract, violation of New York General Business Law ("NY GBL") § 349, violation of NY GBL § 899-aa, violation of the New Jersey Consumer Fraud Act, violation of the New Jersey Data Breach Notification Statute, unjust enrichment, and

declaratory judgment.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, because Plaintiffs and at least one member of the Class, as defined below, is a citizen of a different state than Defendant, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5 million, exclusive of interests and costs.

12. This Court has personal jurisdiction over Defendant because Defendant maintains its principle place of business in this District and conducts a substantial portion of its business in this District.

13. Venue is proper in this Court because the principal place of business of Defendant is in this District. In addition, a substantial part of the events giving rise to the underlying action occurred in this District.

PARTIES

14. Plaintiff Gary Graifman, at all relevant times, is and was a citizen of the State of New Jersey. In or about early 2024, Plaintiff, in connection with registering with Defendant for the ability to potentially bid within an advertised auction Defendant was conducting in New York, was required by Defendant to supply his driver's license information which included full name, address, license number and date of birth.. In or about May 2024, Plaintiff received notification via email from

Defendant that his data had been included in the data breach event that impacted his personal data, including his driver's license information.

15. Defendant Christie's Inc. is a corporation with its principal place of business located at 20 Rockefeller Plaza, New York, New York 10020.

BACKGROUND

Defendant's Business

16. Defendant is one of the world's oldest and largest auction houses, first established in Britain in 1766. Defendant is best known for the sale of art, but also provides business and consulting services to tens or hundreds of thousands of clients worldwide.

17. Defendant describes itself as "a world-leading art and luxury business with a physical presence in 46 countries throughout the Americas, Europe, Middle East, and Asia Pacific, and flagship international sales hubs in New York, London, Hong Kong, Paris and Geneva."[6] In addition to fine art, Defendant's auctions sell rarer wines, jewelry, and collectibles.

18. Defendant regularly conducts auctions at its headquarters in New York, such as the one in which Plaintiff registered to participate.

19. Defendant further advertises that, "[r]enowned and trusted for [its] expert live and online-only auctions, as well as bespoke Private Sales, Christie's

[6] *About Christie's*, Christie's, https://www.christies.com/en/about/overview (last visited Jun. 19, 2024).

unparalleled network of specialists offers our clients a full portfolio of global services, including art appraisal, art financing, international real estate and education. Christie's auctions span more than 80 art and luxury categories, at price points ranging from $500 to over $100 million."[7]

20. As part of its standard business operations, Defendant requires customers to provide documentation confirming their identities, and retains this sensitive PII on their network. This sensitive PII is stored and accessible in their New York headquarters.

21. In its Privacy Notice, Christie's states: "We understand that your personal information is important and we are committed to treating it with the utmost care and security. We have multiple layers of security technologies and controls in our environment which safeguard your data, while at rest or in transit, from unauthorized access or disclosure. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality. In addition, our colleagues receive data protection training and we have in place detailed security and data protection policies which colleagues are required to follow when handling personal information. In an ever-altering threat landscape, we are constantly assessing our security defenses to

[7] *Id.*

ensure your data continues to stay protected. We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so."[8]

22. Because of the highly sensitive and personal nature of the information Christie's acquires and stores, Christie's, upon information and belief, promises to, among other things: keep individuals' Private Information private; comply with industry standards related to data security and the maintenance of Private Information; inform individuals of its legal duties relating to data security and comply with all federal and state laws protecting individuals' Private Information; only use and release individuals' Private Information for reasons that relate to the services it provides; and provide adequate notice to affected individuals if their Private Information is disclosed without authorization.

23. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Christie's assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure and exfiltration.

24. Plaintiff and Class Members relied on Christie's to keep their Private Information confidential and securely maintained and to only make authorized

[8] *Privacy Notice*, Christie's, https://www.christies.com/en/privacy-centre/privacy-notice/overview (last visited Jun. 19, 2024).

disclosures of this information, which Defendant ultimately failed to do.

The Christie's Data Breach

25. On May 9, 2024, according to the Data Breach Notice, Defendant discovered that cybercriminals had gained unauthorized access to its network. Through this unauthorized access, the cybercriminals accessed and downloaded the highly sensitive PII of Defendant's customers.

26. On or about May 30, 2024, Defendant sent the Data Breach Notice out via email to the victims of the Data Breach. The Data Breach Notice stated that:

> On 9 May 2024, we discovered that an unauthorised third party had managed to gain access to Christie's IT network for a limited period of time.
>
> Our teams worked to revoke all access, isolate our systems, and ensure that our network was secure. We immediately appointed additional cyber security experts to investigate this matter on our behalf.
>
> From these investigations, we became aware that during the period of unauthorised access, the third party downloaded a limited amount of client data from Christie's internal client verification system. This system houses verification information relating to client ID checks, which we are required to retain for compliance reasons.

27. With regard to the nature of the stolen information, the Data Breach Notice stated that:

> The impacted personal data was data shown on the photographic identification that you provided to Christie's in the course of our routine client verification procedures.
>
> For Passports: the impacted data was the information shown on the ID page, including full name, gender, passport number,

> expiry date, date of birth, birth place, and MRZ (the machine-readable code at the bottom of the identity page at the beginning of a passport). **Photos and signatures were not exposed.**
>
> For other forms of ID (such as driving licences and National Identity cards): the impacted data was the data shown on the front of the document, for example, full name, date of birth, country, and document number. **Again, photos and signatures were not exposed.**

28. Defendant had obligations created by contracts, industry standards, common law, and representations made to Plaintiff and Class Members to keep their PII secure and confidential, and to protect it from unauthorized access and disclosure. Plaintiff and Class Members provided their PII to Defendant with the reasonable expectation and mutual understanding that Defendant would keep such information protected in accordance with these obligations.

29. As cyberattacks and data breaches have become considerably more frequent in recent years, Defendant knew or should have known that it was likely to be a target for a data breach. Defendant had previously been targeted in August of 2023 by cybercriminals who accessed the GPS locations of a number of collections that would be sold at upcoming auctions.[9] However, despite this prior attack and the increasing likelihood of further cyberattacks, Defendant failed to take reasonable measures to prevent a data breach and protect the highly sensitive PII of its

[9] Scott Ikeda, *Cyber Attack on Christie's Shifted Bidding for $578 Million Worth of Art Auctions Offline*, CPO Magazine (May 17, 2024) https://www.cpomagazine.com/cyber-security/cyber-attack-on-christies-shifted-bidding-for-578-million-worth-of-art-auctions-offline/.

customers.

Defendant Failed to Comply with FTC Guidelines

30. The Federal Trade Commission ("FTC") regularly promulgates guidelines for businesses which highlight the necessity of implementing reasonable data security practices. According to the FTC, the need for data security should factor into all business decision-making.

31. For example, in 2016, the FTC updated its published guidelines, Protecting Personal Information: A Guide for Business, which laid out standard and accepted cyber-security measures for businesses to implement to protect consumers' private data. The guidelines advise businesses, inter alia, to: encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[10]

32. The FTC's guidelines further advise businesses: not to maintain PII longer than necessary for authorization of a transaction; to limit access to sensitive data; to require complex passwords to be used on networks; to use industry-tested methods for security; to monitor for suspicious activity on the network; and to verify that third-party service providers have implemented reasonable security measures.

33. To underscore the binding significance of the promulgated guidance, the FTC has brought enforcement actions against businesses for failing to adequately

[10] Protecting Personal Information: A Guide for Business, FEDERAL TRADE COMMISSION (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

and reasonably protect customer data, pursuant to Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further identify the measures businesses must take to meet their data security obligations consistent with federal law.

34. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

35. Defendant was at all times fully aware of its obligations to protect the Private Information of customers. Defendant was also aware of the significant repercussions that would result from their failure to do so.

Defendant Failed to Comply with Industry Standards

36. In light of the evident threat of cyberattacks seeking consumers' Private Information, several best practices have been identified by regulatory agencies and experts that, at a minimum, should be implemented by business who acquire and retain their customers' Private Information, including but not limited to: educating and training all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; monitoring and limiting the network ports; protecting web browsers and email management systems; and limiting which employees can access sensitive data.

37. On information and belief, Defendant failed to meet the minimum

standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

38. These foregoing frameworks are existing and applicable industry standards in the Defendant's industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the Data Breach

Defendant Knew or Should Have Known that Cybercriminals Would Target Their Customers' PII

39. The FTC hosted a workshop to discuss "informational injuries," which are injuries that consumers like Plaintiff and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.[11] Exposure of highly sensitive personal information that a consumer wishes to keep private may cause harm to the consumer, such as the ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

[11] *FTC Information Injury Workshop, BE and BCP Staff Perspective*, Federal Trade Commission (October 2018) https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf.

40. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

41. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

42. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very

valuable to hackers and identity thieves as it allows them to access users' other accounts.

43. Thus, even if certain information were not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiff's and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiff and Class Members.

44. One such example of this is the development of "Fullz" packages, complete dossiers on individuals which are created by Cybercriminals cross-referencing two sources of the Private Information compromised in the Data Breach to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy. The development of "Fullz" packages means that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other sources and identifiers.

45. In other words, even if certain information such as emails, phone numbers, or credit card or financial account numbers may not be included in the Private Information stolen in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of

fact, including this Court or a jury, to find that Plaintiff and other Class Members' stolen Private Information are being misused, and that such misuse is fairly traceable to the Data Breach.

46. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[12] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

47. Identity thieves can also use stolen PII for a variety of crimes, including credit card fraud, phone or utilities fraud, bank fraud, to obtain a driver's license or official identification card in the victim's name but with the thief's picture, to obtain government benefits, or to file a fraudulent tax return using the victim's information. In addition, identity thieves may rent housing in the victim's name, or even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

[12] *See IdentityTheft.gov*, Federal Trade Commission https://www.identitytheft.gov/Steps (last visited Jun. 19, 2024).

48. PII is data that can be used to detect a specific individual. PII is a valuable property right. Its value is axiomatic, considering the value of big data in corporate America and the consequences of cyber thefts (which include heavy prison sentences). Even this obvious risk-to-reward analysis illustrates beyond doubt that PII has considerable market value.

49. The U.S. Attorney General stated in 2020 that consumers' sensitive personal information commonly stolen in data breaches "has economic value."[13] The increase in cyberattacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendant's industry.

50. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, PII can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[14] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web and that a fullz package sold for $30 in 2017.[15]

---

[13] *Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax*, U.S. Dep't of Justice (Feb. 10, 2020) https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-four-members-china-s-military.

[14] *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends (Oct. 16, 2019) https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.

[15] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian (Dec. 6, 2017) https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

51. Furthermore, even information such as names, email addresses and phone numbers, can have value to a hacker. Beyond things like spamming individuals, or launching phishing attacks using their names and emails, hackers, inter alia, can combine this information with other hacked data to build a more complete picture of an individual. It is often this type of piecing together of a puzzle that allows hackers to successfully carry out phishing attacks or social engineering attacks. This is reflected in recent reports, which warn that "[e]mail addresses are extremely valuable to threat actors who use them as part of their threat campaigns to compromise accounts and send phishing emails."[16]

52. The Dark Web Price Index of 2022, published by PrivacyAffairs shows how valuable just email addresses alone can be, even when not associated with a financial account. The average dark web price in 2022 for 10 million USA email addresses was $120.[17]

53. Beyond using email addresses for hacking, the sale of a batch of illegally obtained email addresses can lead to increased spam emails. If an email address is swamped with spam, that address may become cumbersome or impossible to use, making it less valuable to its owner.

54. Likewise, the value of PII is increasingly evident in our digital

[16] *See* https://www.magicspam.com/blog/dark-web-price-index-the-cost-of-email-data/ (last visited Jun. 19, 2024).

[17] *See* https://www.privacyaffairs.com/dark-web-price-index-2022/ (last visited Jun. 19, 2024).

economy. Many companies, including Defendant, collect PII for purposes of data analytics and marketing. These companies collect it to better target individuals and share it with third parties for similar purposes.

55. One author has noted: "Due, in part, to the use of PII in marketing decisions, commentators are conceptualizing PII as a commodity. Individual data points have concrete value, which can be traded on what is becoming a burgeoning market for PII."[18]

56. Consumers also recognize the value of their personal information and offer it in exchange for goods and services. The value of PII can be derived not only by a price at which consumers or hackers actually seek to sell it, but rather by the economic benefit consumers derive from being able to use it and control the use of it.

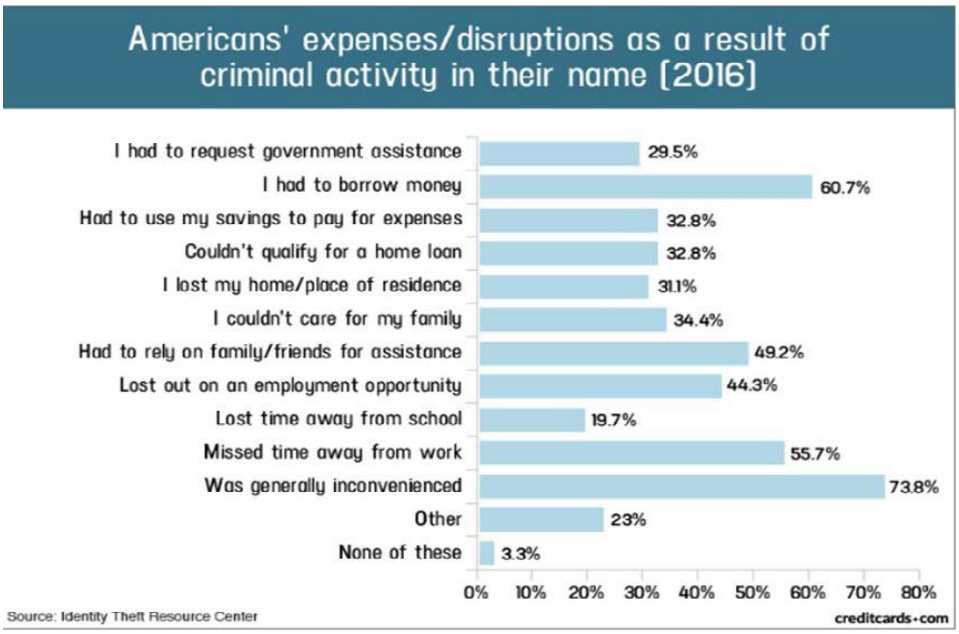
57. A consumer's ability to use their PII is encumbered when their identity or credit profile is infected by misuse or fraud. For example, a consumer with false or conflicting information on their credit report may be denied credit. Also, a consumer may be unable to open an electronic account where their email address is already associated with another user. In this sense, among others, the theft of PII in the Data Breach led to a diminution in value of the PII.

58. Data breaches, like that at issue here, damage consumers by interfering

[18] John T. Soma, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ('PII') Equals the "Value" of Financial Assets*, 15 Rich. J. L. & Tech. 11, 14 (2009).

with their fiscal autonomy. Any past and potential future misuse of Plaintiff's PII impairs their ability to participate in the economic marketplace.

59. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of PII:[19]



60. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or personal financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[20]

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used

[19] Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (Jun. 11, 2021) https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/.

[20] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), available at https://www.gao.gov/products/gao-07-737 (last visited Jun. 19, 2024).

> to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

61. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for years.

62. As a result, Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

CLASS ACTION ALLEGATIONS

63. Plaintiff brings this case as a class action pursuant to Fed. R. Civ. P. 23 on behalf of a Nationwide Class and a New Jersey Subclass defined as:

The Nationwide Class is defined as:

> All individuals in the United States who had Private Information accessed and/ or acquired as a result of the Data Breach reported by Christie's in May 2024, including all who were sent a notice of the Data Breach

The New Jersey Subclass is defined as:

> All residents of New Jersey who had Private Information accessed and/ or acquired as a result of the Data Breach reported by Christie's in May 2024, including all who were sent a notice of the Data Breach.

64. Excluded from the Class and Subclass are Defendant, its agents,

affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any of Defendant's officers or directors, any successors, and any judge who adjudicates this case, including their staff and immediate family.

65. Plaintiff reserves the right to amend the class and subclass definitions.

66. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

a. **Numerosity**. The members of the Class and Subclass are so numerous that joinder would be impracticable. The exact number of class members is unknown to Plaintiff, but on information and belief, consists of over 500,000 individuals who are current or former customers of Defendant.

b. **Ascertainability**. The identities of Class Members are ascertainable through Defendant's records, Class Members' records, publication notice, self-identification, and other means.

c. **Typicality**. Plaintiff's claims are typical of class and subclass claims as each arises from the same factual and legal theories.

d. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's and Subclass's interests. His interests do not conflict with the Class's and Subclass's interests, and he has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Commonality**. Plaintiff's and the Class's and Subclass's claims raise predominantly common factual and legal questions that a class-wide proceeding can answer for the Class and Subclass. Indeed, it will be necessary to answer the following questions, which include but are not limited to:

i. Whether Defendant had a duty to use reasonable care in protecting its computer network from the Data Breach;

ii. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

iii. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations.

iv. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

v. Whether Defendant knew or should have known that their data security systems and monitoring processes were deficient;

vi. Whether Defendant was negligent in maintaining, protecting, and securing its computer systems;

vii. Whether Defendant should have discovered the Data Breach sooner;

viii. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

ix. Whether Defendant's response to the Breach was reasonable;

x. Whether Defendant's breach of its duty to implement reasonable security systems directly and/or proximately caused damages to Plaintiffs and Class Members;

xi. Whether Defendant adequately addressed and fixed the vulnerabilities that enabled the Data Breach;

xii. Whether Defendant breached contracts with Plaintiff and Class Members;

xiii. Whether Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class Members;

xiv. Whether Defendant failed to provide notice of the Data Breach in a timely and adequate manner; and

xv. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

67. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The

damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

COUNT I
Negligence

68. Plaintiff incorporates by reference and realleges each and every allegation contained above, as though fully set forth herein. Plaintiff asserts this claim on behalf of himself and the Nationwide Class.

69. At all times relevant hereto, Defendant owed Plaintiff and Class Members a duty to act with reasonable care to ensure the security and continuity of its networks and systems. Defendant assumed this obligation and owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the network and systems from attack by malicious actors.

70. Plaintiff and Class Members are a well-defined, foreseeable, and probable group of victims that Defendant was aware, or should have been aware, could be injured by inadequate data security measures.

71. Defendant's duty of care to use reasonable and adequate security measures arose as a result of Defendant's role as a provider of goods and services to clientele as recognized by laws and regulations including but not limited the FTC Act and common law. Defendant was in a superior position to ensure that its security

measures were sufficient to protect against the foreseeable risk of harm to Plaintiff and Class Members from a data breach.

72. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair... practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

73. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential private information.

74. Defendant breached its duties and was negligent by failing to use reasonable measures to protect its systems from a Data Breach. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain reasonable and adequate security measures to safeguard its networks, systems, and servers;

b. Failing to adequately monitor the security of its networks and systems;

c. Failing to ensure that its email systems had reasonable data security safeguards in place;

d. Failing to have in place reasonable and adequate mitigation policies and procedures;

e. Failing to detect in a timely manner that there had been an exploitation of its security vulnerabilities; and

f. Failing to notify Plaintiff and Class Members about the Data Breach in a timely and adequate fashion so that they could take appropriate steps to mitigate the potential harm.

75. It was foreseeable that Defendant's failure to use reasonable measures to protect its networks and systems would result in injury to Plaintiff and Class Members. Furthermore, the breach of security was reasonably foreseeable given the well-known high frequency of cyberattacks and data breaches in recent years.

76. It was therefore foreseeable that the failure to adequately secure the Private Information stored in their systems and networks would result in one or more types of injuries to Plaintiff and Class Members, including the financial injury that resulted.

77. Defendant's conduct was grossly negligent and departed from reasonable standards of care, including but not limited to, failing to adequately protect their systems and networks from a cyberattack.

78. Neither Plaintiff nor Class Members contributed to the Data Breach and subsequent harm endured as a result of the Data Breach.

79. Plaintiff and Class Members are also entitled to injunctive relief

requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) compensate Plaintiff and Class Members for all financial losses suffered.

80. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that it was failing to meet their duties, and that Defendant's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the Data Breach.

81. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

COUNT II
Negligence per se

82. Plaintiff incorporates by reference and realleges each and every allegation contained above, as though fully set forth herein. Plaintiff asserts this claim on behalf of himself and the Nationwide Class.

83. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as Defendant for failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's

duty.

84. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with the industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of this Data Breach.

85. Defendant's violation of Section 5 of the FTC Act constitutes negligence per se.

86. Plaintiff and Class Members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

87. Moreover, the harm that has occurred is the type of harm that the FTC Act was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members.

88. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have been injured as described herein and above, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

COUNT III
Breach of Contract

89. Plaintiff incorporates by reference and realleges each and every

allegation contained above, as though fully set forth herein. Plaintiff asserts this claim on behalf of himself and the Nationwide Class.

90. [Discuss GG contract with Christie's]

COUNT IV
Breach of Implied Contract

91. Plaintiff incorporates by reference and realleges each and every allegation contained above, as though fully set forth herein. Plaintiff asserts this claim on behalf of himself and Nationwide Class, as an alternative to the claim for Breach of Contract above (Count III).

92. Plaintiff and Class Members were required deliver their PII to Defendant as part of the process of obtaining services provided by Defendant. Plaintiff and Class Members paid money, or money was paid on their behalf, to Defendant in exchange for services.

93. Defendant solicited, offered, and invited Class Members to provide their PII as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their PII to Defendant.

94. Defendant accepted possession of Plaintiff's and Class Members' PII for the purpose of providing services to Plaintiff and Class Members.

95. Plaintiff and the Class entrusted their PII to Defendant. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such

information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

96. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations (including FTC guidelines on data security) and were consistent with industry standards.

97. Implicit in the agreement between Plaintiff and Class Members and the Defendant to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses, (f) retain the PII only under conditions that kept such information secure and confidential.

98. The mutual understanding and intent of Plaintiff and Class Members on the one hand, and Defendant, on the other, is demonstrated by their conduct and course of dealing.

99. On information and belief, at all relevant times Defendant promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiff and Class Members that it would only disclose PII under certain circumstances, none of which relate to the Data Breach.

100. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiff's and Class Members' PII would remain protected.

101. Plaintiff and Class Members paid money to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

102. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

103. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

104. Every contract in this State has an implied covenant of good faith and fair dealing, which is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

105. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

106. Defendant breached the implied contracts it made with Plaintiff and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiff and the Class once the relationship ended, and by failing to provide accurate notice to them that personal information was

compromised as a result of the Data Breach.

107. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard PII, failing to timely and accurately disclose the Data Breach to Plaintiff and Class Members and continued acceptance of PII and storage of other personal information after Defendant knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach.

108. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiff and Class Members sustained damages, including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

109. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

110. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT V
Violation of the New York Deceptive Trade Practices Act ("GBL")
New York Gen. Bus. Law § 349

111. Plaintiff incorporates by reference and realleges each and every allegation contained above, as though fully set forth herein. Plaintiff asserts this claim on behalf of himself and the Nationwide Class.

112. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and furnishing of services, in violation of N.Y. Gen. Bus. Law § 349(a), including but not limited to the following:

(1) Misrepresenting material facts to Plaintiff and the Class by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Class Members' PII from unauthorized disclosure, release, data breaches, and theft;

(2) Misrepresenting material facts to Plaintiff and the Class by representing that they did and would comply with the requirements of federal and state laws pertaining to the privacy and security of Class Members' PII;

(3) Omitting, suppressing, and/or concealing material facts of the inadequacy of its privacy and security protections for Class Members' PII;

(4) Engaging in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Class Members' PII, in violation of duties imposed by and public policies reflected in applicable federal and state laws; and,

(5) Engaging in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Data Breach to the Class in a timely and accurate manner, contrary to the duties imposed by N.Y. Gen. Bus. Law § 899-aa(2).

113. Defendant knew or should have known that its network and data security practices were inadequate to safeguard the PII entrusted to it by Class Members, and that risk of a data breach or theft was highly likely.

114. Defendant should have disclosed this information because Defendant was in a superior position to know the true facts related to the defective data security and made affirmative representations regarding its data security commitments and practices.

115. Defendant's failure constitutes false and misleading representations, which have the capacity, tendency, and effect of deceiving or misleading consumers (including Plaintiff and Class Members) regarding the security of Defendant's

network and aggregation of PII.

116. The representations upon which current and former customers (including Plaintiff and Class Members) relied were material representations (e.g., as to Defendant's adequate protection of PII), and current and former customers (including Plaintiff and Class Members) relied on those representations to their detriment.

117. Defendant's conduct is unconscionable, deceptive, and unfair, as it is likely to, and did, mislead consumers acting reasonably under the circumstances. As a direct and proximate result of Defendant's conduct, Plaintiff and other Class Members have been harmed, in that they were not timely notified of the Data Breach, which resulted in profound vulnerability to their personal information.

118. Defendant knew or should have known that their computer systems and data security practices were inadequate to safeguard Class Members' PII and that the risk of a data security incident was high.

119. Defendant's acts, practices, and omissions were done in the course of advertising and conducting Defendant's regular business in the State of New York.

120. As a direct and proximate result of Defendant's unconscionable, unfair, and deceptive acts and omissions, Plaintiff's and Class Members' PII was disclosed to third parties without authorization, causing and will continue to cause Plaintiff and Class Members damages.

121. Plaintiff and Class Members would not have obtained services at

Defendant had they known the true nature and character of Defendant's data security practices. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of promises that Defendant would keep their information reasonably secure, and in the absence of the promise to monitor their computer systems and networks to ensure that they adopted reasonable data security measures.

122. As a direct and proximate result of Defendant's multiple, separate violations of GBL §349, Plaintiff and the Class Members suffered damages including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

123. As a result, Plaintiff and the Class Members have been damaged in an amount to be proven at trial.

124. Plaintiff brings this action on behalf of himself and Class Members for

the relief requested above and for the public benefit to promote the public interests in the provision of truthful, fair information to allow consumers to make informed decisions and to protect Plaintiff, Class Members and the public from Defendant's unfair, deceptive, and unlawful practices. Defendant's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

125. Plaintiff and Class Members seek relief under N.Y. Gen. Bus. Law § 349(h), including, but not limited to, actual damages, treble damages, statutory damages, injunctive relief, and/or attorney's fees and costs.

126. On behalf of himself and other members of the Class, Plaintiff seeks to enjoin the unlawful acts and practices described herein, to recover his actual damages or fifty dollars, whichever is greater, three times actual damages, and reasonable attorneys' fees.

127. Also as a direct result of Defendant's violation of GBL § 349, Plaintiff and the Class Members are entitled to damages as well as injunctive relief, including, but not limited to, ordering Defendant to: (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT VI
Violation of New York Gen. Bus. Law § 899-aa

128. Plaintiff incorporates by reference and realleges each and every

allegation contained above, as though fully set forth herein. Plaintiff asserts this claim on behalf of himself and the Nationwide Class.

129. According to the Data Breach Notice, Defendants identified the ransomware incident on May 9, 2024. However, Defendants did not notify Plaintiff and Class Members of the Data Breach until May 30, 2024.

130. Pursuant to Gen. Bus. Law § 899-aa(2), Defendants were required to provide disclosure to the victims of a data breach within "the most expedient time possible and without unreasonable delay. . . ."

131. Defendants violated the statute by waiting three weeks to notify Plaintiff and Class Members of the data breach.

132. As a result of Defendants' unwarranted and unreasonable delay in notifying the data breach victims, the victims were unaware that their Private Information had been illegally accessed and stolen and that they were at drastically increased risk of being subject to identity theft. Had they known sooner, they could have taken immediate steps to protect their identities and prevent further injury.

133. As a result of the Defendants' violation of the statute, Plaintiff and Class Members were injured and demand all remedies warranted by law.

COUNT VII
Violation Of The New Jersey Consumer Fraud Act
(N.J. Stat. Ann. § 56:8-1 et seq.)

134. Plaintiff incorporates by reference and realleges each and every allegation contained above, as though fully set forth herein. Plaintiff asserts this

claim on behalf of himself and the New Jersey Subclass.

135. Defendant is a "person" within the meaning of N.J. Stat. Ann. § 56:8-1(d).

136. The New Jersey Consumer Fraud Act, N.J. Stat. §§ 56:8-1, et seq., prohibits unconscionable commercial practices, deception, fraud, false pretense, false promise, misrepresentation, as well as the knowing concealment, suppression, or omission of any material fact with the intent that others rely on the concealment, omission, or fact, in connection with the sale or advertisement of any merchandise.

137. In the course of advertising its services to Plaintiff and Subclass Members, Defendant represented that it would adequately secure the sensitive private information of Plaintiff and Subclass Members, and/or omitted that it did not have all required and industry-standard security measures in place to protect this sensitive information.

138. Defendant's misrepresentations and omissions were likely to deceive reasonable customers. Had Plaintiff and Subclass Members known that Defendant did not have reasonable security measures in place to protect the sensitive information stored and processed within its servers and systems, they would not have contracted with Defendant.

139. Defendant intended to mislead Plaintiff and Subclass Members and induce them to rely on their misrepresentations and omissions.

140. Defendant acted intentionally, knowingly, and maliciously to violate

New Jersey's Consumer Fraud Act, and recklessly disregarded Plaintiff's and Subclass Members' rights.

141. As a direct and proximate result of Defendant's unconscionable and deceptive practices, Plaintiff and Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages.

142. Plaintiff and Subclass Members seek all monetary and non-monetary relief allowed by law, including injunctive relief, other equitable relief, actual damages, treble damages, restitution, and attorneys' fees, filing fees, and costs.

COUNT VIII
Violation of the New Jersey Data Breach Notification Statute
N.J. Stat. Ann. § 56:8-163

143. Plaintiff incorporates by reference and realleges each and every allegation contained above, as though fully set forth herein. Plaintiff asserts this claim on behalf of itself and the New Jersey Subclass.

144. New Jersey law requires that any business that conducts business in New Jersey and maintains computerized records of Personal Information must disclose a breach following discovery of that breach to New Jersey residents "in the most expedient time possible and without unreasonable delay." N.J. Stat. Ann. §56:8-163(a). This mandate is necessary so that victims of the breach may take steps to safeguard their identities as quickly as possible and preempt any attempts by data thieves to commit crimes associated with identity theft.

145. "Personal Information" in this statute is defined as:

> an individual's first name or first initial and last name linked with any one or more of the following data elements: (1) Social Security number; (2) driver's license number or State identification card number; (3) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; or (4) user name, email address, or any other account holder identifying information, in combination with any password or security question and answer that would permit access to an online account.

As Plaintiff's and Subclass Members' full names and driver's license numbers or state identification card numbers were illegally accessed and exfiltrated in the Data Breach, Defendant is liable for failing to comply with this statute.

146. According to the Data Breach Notice, Defendants identified the ransomware incident on May 9, 2024. However, Defendants did not notify Plaintiff and Class Members of the Data Breach until May 30, 2024. Defendants violated the statute by waiting three weeks to notify Plaintiff and Class Members of the data breach.

147. As a result of Defendants' unwarranted and unreasonable delay in notifying the data breach victims, the victims were unaware that their Personal Information had been illegally accessed and stolen and that they were at drastically increased risk of being subject to identity theft. Had they known sooner, they could have taken immediate steps to protect their identities and prevent further injury.

148. As a result of the Defendants' violation of the statute, Plaintiff and

Class Members were injured and demand all remedies warranted by law.

COUNT IX
Unjust Enrichment

149. Plaintiff incorporates by reference and realleges each and every allegation contained above, as though fully set forth herein. Plaintiff asserts this claim on behalf of itself and the Nationwide Class, as an alternative to the claim for Breach of Contract above (Count III).

150. Upon information and belief, Defendant funds any data security measures it implements entirely from its general revenue, including from money they make based upon representations of Protecting Plaintiff's and Class Members' Private Information.

151. There is a direct nexus between money paid to Defendant and the requirement that Defendant adequately secure their computer networks and adopt sufficient data security practices to safeguard and protect Private Information.

152. Plaintiff and Class Members paid Defendant a certain sum of money, which was used to fund any data security measures implemented by Defendant via contracts with Defendant.

153. As such, a portion of the payments made by or on behalf of Plaintiff and Class Members is to be used to provide a reasonable and adequate level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

154. Plaintiff and Class Members directly and indirectly conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and/or its agents and provided Defendant with their sensitive PII. In exchange, Plaintiff and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their PII protected with adequate data security.

155. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the money paid by Plaintiff and Class Members for business purposes.

156. Defendant enriched itself by saving the costs they reasonably should have expended on adequate data security measures to secure its servers and networks. Instead of providing a reasonable and adequate level of security that would have prevented the Data Breach, Defendant instead chose to shirk their data security obligations to increase profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective data security measures. Plaintiff and Class Members suffered as a direct and proximate result of Defendant's calculated failures to provide the requisite reasonable and adequate data security.

157. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement reasonable and adequate data management and security measures that are mandated by federal law and industry standards.

158. Defendant acquired the monetary benefit and Private Information through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

159. Plaintiff and Class Members have no complete adequate remedy at law.

160. As a direct and proximate result of Defendant's misconduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

161. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for its services.

COUNT VI
CLAIM FOR DECLARATORY & INJUCTIVE RELIEF

162. Plaintiff incorporates by reference and realleges each and every allegation contained above, as though fully set forth herein. Plaintiff asserts this claim on behalf of itself and the Nationwide Class.

163. Under the Declaratory Judgment Act, 28 U.S.C. § 2201 *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal laws and regulations described in this complaint.

164. An actual controversy has arisen in the wake of the Data Breach at issue regarding Defendant's common law and other duties to act reasonably with respect to safeguarding customers' sensitive PII. Plaintiff alleges Defendant's actions in this respect were inadequate and unreasonable and, upon information and belief, remain inadequate and unreasonable. Additionally, Plaintiff and the Class continue to suffer injury due to the continued and ongoing threat to their sensitive Private Information.

165. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owed, and continues to owe, a legal duty to provide reasonable and adequate protection for its customers' PII;

b. Defendant's failure to properly secure its computer network has damaged Plaintiff and Class Members as described above;

c. Defendant owed, and continues to owe, a legal duty to secure the sensitive information with which it is entrusted, and to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

d. Defendant breached, and continues to breach, its legal duty by failing to employ reasonable measures to secure customers' personal and financial information; and

e. Defendant's breach of its legal duty continues to cause harm to Plaintiff and the Class.

166. The Court should also issue corresponding injunctive relief requiring Defendant to employ adequate security protocols consistent with industry standards to protect their clients' data.

167. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another breach of Defendant's data system. If another breach of Defendant's data system occurs, Plaintiff and the Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified in full, and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiff and the Class for their out-of-pocket and other damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiff and the Class.

168. The hardship to Plaintiff and the Class if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiff and Class Members will likely be subjected to further monetary harm and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

169. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the injuries that would result to Plaintiff, the

Class, and the public at large.

PRAYER FOR RELIEF

Plaintiff and the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class and Subclass, appointing Plaintiff as class and subclass representative, and appointing his counsel to represent the Class;

B. Awarding declaratory, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Defendant from further violations of statutes and common law that would further damage Plaintiff and the Class;

E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

Respectfully submitted, this 29th day of July, 2024.

Respectfully submitted,

/s/ Howard Longman

Howard T. Longman
LONGMAN LAW, P.C.
354 Eisenhower Parkway, Suite 1800
Livingston, New Jersey 07039
Telephone: (973) 994-2315
hlongman@longman.law